Abb. 1: Typischer Arbeitsplatz in einer Leitzentrale

Quelle: Nowega GmbH

Sicherheit bei der Steuerung von Gasversorgungsnetzen

Die sichere und kontinuierliche Versorgung von Bevölkerung und Industrie mit Erdgas wird im Wesentlichen durch Leitzentralen sichergestellt, welche rund um die Uhr besetzt sind. Entsprechend wichtig ist deshalb die technische wie auch die organisatorische Sicherheit dieser Knotenpunkte der Gasversorgung. Mögliche Stör- und Bedrohungsszenarien können in diesem Fall z. B. die Unterbrechung der physischen Datenanbindung, aber auch Cyber-Angriffe auf die Infrastruktur der Gasversorgung sein. Der Beitrag beschreibt verschiedene Maßnahmen und Sicherheitsmechanismen zum Schutz der Leitstellen vor diesen Szenarien.

von: Dr. Werner Rott, Lara Berdelsmann (beide: GASCADE Gastransport GmbH) & Svend Wortmann (Nowega GmbH)

Der Primärenergieverbrauch von Erdgas in der Bundesrepublik Deutschland ist mit rund 3.230 Petajoule (PJ), umgerechnet 897 Terawattstunden (TWh) [1] deutlich höher als der deutsche Stromverbrauch, der sich auf insgesamt 520 TWh beläuft [2]. Beide Energieformen sind an Leitungsnetze gebunden und müssen der Bevölkerung ununterbrochen zur Nutzung bereitgestellt werden.

Einen wesentlichen Beitrag zu dieser allgemeinen Versorgung mit Energie wird in den Leitzentralen wahrgenommen (**Abb. 1**). Diese sind 24 Stunden am Tag, sieben Tage die Woche und 365 Tage im Jahr mit Dispatchern besetzt. Diese gewährleisten mit ihrer Arbeit u. a. die Netzstabilität. Entsprechend wichtig ist deshalb die technische und organisatorische Sicherheit der Erdgas-Leitstellen, die im Zentrum dieses Beitrags steht. Eine umfangreichere Darstellung findet sich in der DVGW-Information GAS Nr. 6 „Dispatching im Gasversorgungsnetz“, in dem DVGW-Merkblatt DVGW G 1001 „Sicherheit in der Gasversorgung; Risikomanagement von gastechnischen Infrastrukturen im Normalbetrieb“ sowie in weiteren einschlägigen DVGW-Veröffentlichungen.

Redundanzkonzept – Fallback-Optionen bei Ausfällen

Die Versorgung der Leitzentrale mit Daten aus dem Feld und die sichere Ansteuerung von Netzelementen und Komponenten aus der Leitzentrale heraus sind wesentliche Voraussetzungen für ein reibungsloses Dispatching; hierfür ist im Wesentlichen das sogenannte SCADA-System (Supervisory Control and Data Acquisition) zuständig **(Abb. 2)**. An zweiter Stelle der Anforderungsliste steht die Interpretation der Daten durch Softwareprodukte in der Leitzentrale, welche die Daten visualisieren und Vorschläge für die Steuerung der Gasflüsse machen. Die sichere Versorgung mit Daten und deren Interpretation kann dabei auf verschiedene Weise unterbrochen oder eingeschränkt werden:

- Unterbrechung der physischen Datenanbindung (Kabelbruch),
- Ausfall der Spannungsversorgung (lokaler, flächendeckender Stromausfall) oder
- Cyber-Angriff auf die Leitzentrale bzw. die Unterstationen.

Darüber hinaus können andere Kommunikationswege, die nicht SCADA-basiert sind, ausfallen und dadurch die Abstimmung aus der Leitzentrale mit Stationen in der Gas-Peripherie (z. B. Verdichterstationen) mit anderen Gasversorgern oder – in einer Krisensituation – mit Behörden erschweren oder gar unmöglich machen.

Auf alle hier genannten Ereignisse kann und muss sich ein Netzbetreiber vorbereiten. Dabei muss er – je nach Einschätzung des Risikos – für technische, wirtschaftliche oder materielle Schäden (bis hin zu Personenschäden) Maßnahmen ergreifen, um solche Ereignisse gut vorbereitet meistern zu können; wertvolle Hinweise hierzu bietet beispielsweise das bereits genannte DVGW-Merkblatt G 1001. Im Folgenden wird auf die genannten Störfaktoren näher eingegangen.

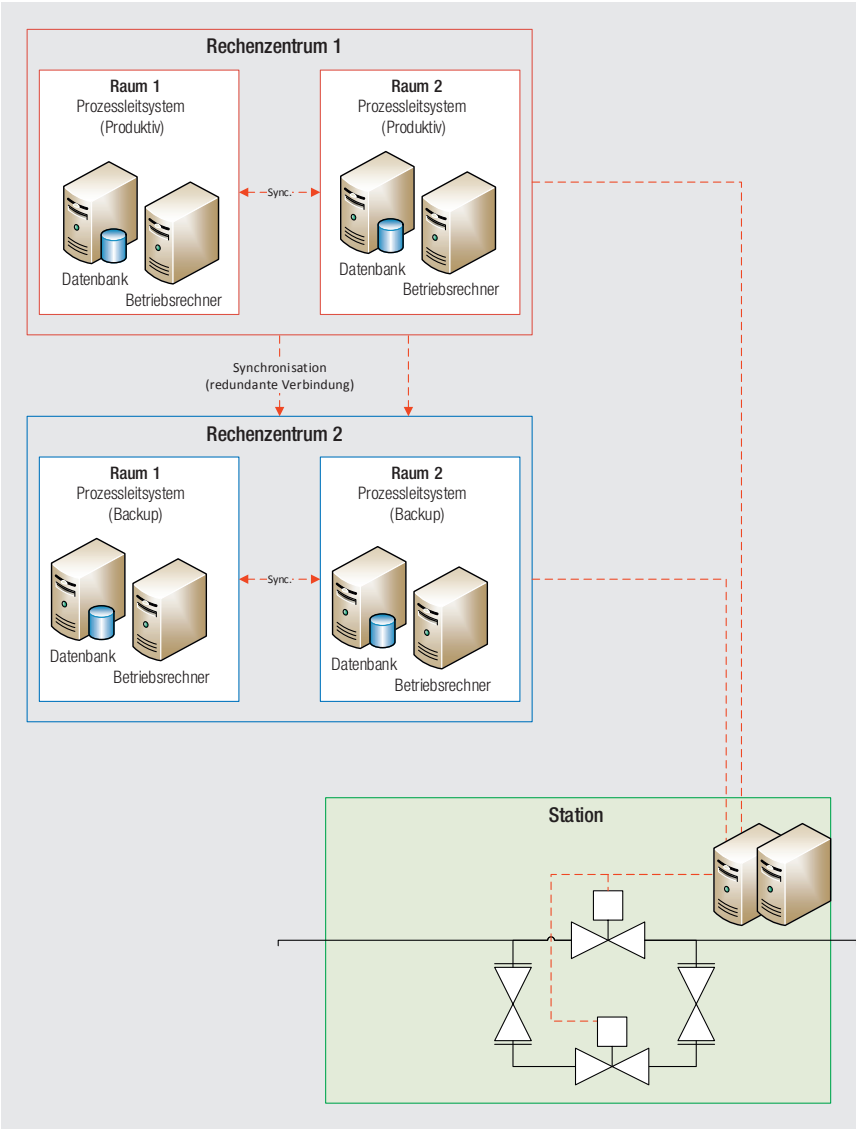
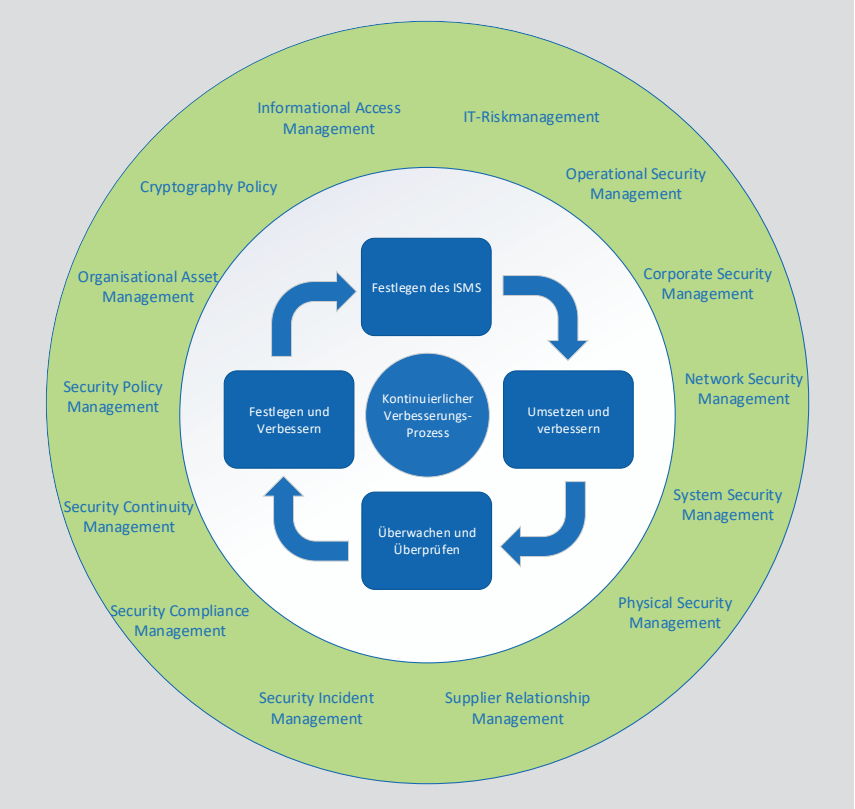


Abb. 2: *Schematischer Aufbau eines Prozessleitsystems*

Unterbrechung der physischen Datenanbindung (Kabelbruch)

Immer wieder kommt es vor, dass Kabelverbindungen zwischen Leitstellen und Feldstationen unterbrochen werden. Grund hierfür ist in den meisten Fällen eine mechanische Beschädigung. Dies trifft vor allem auf Kabel (Lichtwellenleiter- oder Kupferkabel) zu, die nicht im relativen Schutz der Gasrohrleitungen verlegt sind. Tritt so ein Ereignis ein, wird dies in der Leitstelle erkannt und lokalisiert. Die Leitstelle sollte je nach Wichtigkeit der fehlenden Steuerbarkeit der Feldstation(en) in der Lage sein, automatisch oder manuell einen Ersatzweg für die Datenanbindung zu schalten. Hierzu geeignet ist z. B. das öffentliche Telekommunikationsnetz. Wenn der Gasversorger über eigene Kabelanbindungen verfügt, kann die Störung z. B. durch die Umleitung der Daten ab der Schadstelle auf eine unterbrechungsfreie Strecke kompensiert werden.

Sind Ersatzkommunikationswege nicht verfügbar, muss im Dispatching gemeinsam mit dem Betrieb vor Ort entschieden werden, ob und ggf. welche Stationen mit Betriebspersonal besetzt werden müssen. Diese Alarmierung bedarf allerdings noch einer funktionierenden Kommunikation über andere Kommunikationskanäle, weshalb rechtzeitig Pläne und Strategien auch für den Fall erarbeitet werden müssen, wenn die regulären Kommunikationswege nicht mehr zu Verfügung stehen.



Quelle: GASCADE Gastransport GmbH

Abb. 3: *Auf ISMS-Prozesse angewandtes PDCA-Modell*

Hinweise hierzu finden sich u. a. in dem DVGW-Merkblatt G 1003 „Hinweise zur Aufrechterhaltung der sicheren Gasversorgung bei Ausfall der regulären Kommunikation“.

Unterbrechungsfreie Spannungsversorgung

Ein weiterer Grund für den Ausfall der Versorgung der Leitzentralen mit Daten oder gar der Ausfall der Leitzentrale selbst kann die Unterbrechung der Spannungsversorgung sein. Bei der Untersuchung der Risiken eines Spannungsausfalls im Feld und in der Leitzentrale sollten verschiedene räumliche und zeitliche Szenarien der Spannungsunterbrechung untersucht werden.

Lokale, kurzfristige Spannungsunterbrechungen sind – wie alle in diesem Beitrag beschriebenen Ausfälle auch – in Deutschland zwar selten, kommen aber vor. Diese kurzfristigen Stromausfälle können gut mit unterbrechungsfreien Spannungsversorgungen (kurz: USV; meist batteriegepuffert) überbrückt werden. Es empfiehlt sich, USV an allen Stationen vorzusehen. Durch diese Maßnahme ist man im Zeitbereich von Sekunden bis wenige Stunden gut aufgestellt. Die Frage nach der räumlichen Ausdehnung des Spannungsausfalls stellt sich dann auch nicht. Ebenso sollte die Kommunikation über alternative Kommunikationswege in diesem Zeitbereich noch funktionieren, da auch bei den Telekommunikationsverbindungen USV eingesetzt werden.

Untersuchungsintensiver wird das Szenario eines länger andauernden und großflächigen Stromausfalls: Während die Leitzentrale und wesentliche Feldstationen (z. B. Verdichterstationen) neben den USV auch über eine Notstromversorgung verfügen, deren Überbrückungszeit wiederum nur von der Menge des verfügbaren Treibstoffes abhängt, verfügen einige Feldstationen wie Absperrarmaturen oder Gas-Druckregel- und Messanlagen (GDRM-Anlagen) über keine länger verfügbare Notstromversorgung. Auch die USV der Telekommunikations-Anbieter fallen nach wenigen Stunden aus, sodass auch die Kommunikation über die eingeplanten Ersatzwege im Zweifelsfall nicht mehr zur Verfügung steht. Für diesen Fall muss der betroffene Netzbetreiber nun zuerst sicherstellen, dass die Anlagen, die nicht mehr der Kontrolle der Leitstelle unterliegen, in einen sicheren Zustand überführt werden.

Als Nächstes muss dann abgeschätzt werden, wie viel Gas an welcher Übergabestelle noch benötigt wird und ob diese jeweilige Übergabestelle noch autark oder mit entsprechenden Maßnahmen durch die Leitstelle weiter betrieben werden kann. Bei der Abschätzung des verbleibenden Gasabsatzes ist folgender Ausblick wichtig: Der überwiegende Teil der Abnehmer in der Fläche, die über keine Notstromversorgung verfügen, kann kein Gas mehr abnehmen, da ohne Strom der Großteil der Gasverbrauchsgeräte nicht betrieben werden kann.

Cyber-Angriff auf die Leitzentrale oder die Unterstationen

Die Systeme der Leitstellen sind, wie jedes IT-System, Bedrohungen aus zahlreichen Quellen ausgesetzt. Darunter gehören Angriffe durch Hacker, versehentliche oder böswillige Handlungen von Mitarbeitern und Externen bis hin zu organisierter Kriminalität und Aktivitäten von Regierungen.

Im Gegensatz zur traditionellen IT können Angriffe in diesem Bereich, angesichts der Echtzeit-Eigenschaften der Steuerungssysteme, schnell zu kaskadierenden Effekten führen. Von daher erfordern Echtzeit-Steuerungssysteme eine schnellstmögliche Vorfallsreaktion sowie die Identifizierung des initialen Angriffsvektors. Die häufigsten Angriffsvektoren sind hierbei physische Zugriffe (z. B. durch USB-Stick, externe Festplatte oder physischer Zugang an Systemen), gefolgt von externen Zugängen und Fernzugängen zu Wartungszwecken sowie Vorfälle durch Manipulationen in Lieferketten (d. h. geänderte bzw. modifizierte Hardware oder Software, schadhafte Software- und Firmware-Updates, Wartungswerkzeuge bzw. -ausrüstung).

Während physische Vorfälle, beabsichtigt oder nicht, von Mitarbeitern, Dienstleistern, Beratern und Auftragnehmern

ausgelöst werden, sind Remote-Access-Ereignisse überwiegend auf böswillige Hacker zurückzuführen und Lieferketten-Vorfälle auf aktuelle Dienstleister, Berater und sowie die organisierte Kriminalität [3]. Dies impliziert die Notwendigkeit einer verstärkten Schulung zu Sicherheitsbewusstsein, der physischen Perimeterkontrolle, die Umsetzung von stärkeren Richtlinien für die Verwaltung physischer Vermögenswerte, die Identifikation der Anlagen und das Erstellen eines Anlageninventars, die Einsicht in die Topologien der Kontrollsysteme und letztlich die Einführung eines kontinuierlichen Prozesses zur Aufrechterhaltung der Informationssicherheit. Hierbei sind die Normen der ISO 27000-Serie, NIST CSF, NIST 800-Serie und die ISO 62443 im Umfeld der ICS-/SCADA-Systeme die gebräuchlichsten Standards und bieten entsprechende Hilfestellungen.

Sicherheitsmechanismen bei SCADA-Systemen

Die dem Informationssicherheitsmanagement zugrundeliegenden Grundsätze „Vertraulichkeit“ (kein Dritter erlangt Informationen, die er nicht kennen darf), „Integrität“ (Informationen werden nicht unbemerkt/unberechtigterweise verändert) sowie „Verfügbarkeit“ (alle Informationen stehen bei Bedarf zur Verfügung) definieren heute insbesondere auch die Sicherheitsanforderungen an das SCADA-System. Es darf also davon ausgegangen werden, dass ein zertifiziertes ISMS geeignet ist, die Erfüllung dieser wesentlichen Kriterien für die Sicherheit des SCADA-Systems zu überwachen.

Vertraulichkeit:

- physische Sicherheit durch Zutrittskontrolle zu Leitzentrale, Rechenzentren und Stationen durch verschlossene Türen, Zäune, Sicherung der Fenster usw. (Einbruchsicherung)
- Zugangskontrolle durch sichere Passwörter
- Beschränkung des Zugangs auf den Personenkreis, der diesen unbedingt benötigt
- Sicherheit des SCADA-Netzes durch Trennung vom Office-Netz
- Cybersicherheit des SCADA-Systems (Hackerangriffe usw.)

Integrität:

- klar definierte Prozesse
- Mitarbeiterauswahl
- Mitarbeiterschulung/gründliche Einarbeitung
- Beschränkung der Rechte innerhalb des Systems, z. B. Steuerberechtigung nur für Dispatcher

Verfügbarkeit:

- redundante SCADA-Server
- aktuelle und leistungsfähige Systeme
- aktuelle und leistungsfähige Hardware
- regelmäßige Sicherheits-Patches

Als Hilfsmittel, um die Erfüllung dieser Sicherheitskriterien zu überwachen, bietet sich ein Risikomanagementsystem an, welches üblicherweise ohnehin im Rahmen des ISMS im Einsatz ist. Im Anhang des DVGW-Merkblattes G 1001 werden beispielhaft die Elemente eines einfachen Risikomanagementsystems gezeigt. Auf der Basis einer Risiko-Bewertungsmatrix werden Schadensausmaße je nach Schadenstyp in Kategorien eingeteilt. Auch die Eintrittswahrscheinlichkeiten werden in Kategorien eingeteilt. Anschließend werden die identifizierten Risiken nach möglichem Schadensausmaß und Eintrittswahrscheinlichkeit bewertet, dies kann z. B. in Tabellenform erfolgen. Die Wirkung der risikomindernden Maßnahmen lässt sich durch den Vergleich der Risiken ohne und mit Minderungsmaßnahmen darstellen.

Managementsystem für Informationssicherheit (ISMS) – Schutz vor IT-Bedrohungen

Vor dem Hintergrund der aktuellen Sicherheitslage und einer bestehenden Abhängigkeit des Betriebes von Leitzentralen von der Informations- und Kommunikationstechnologie hat die IT-Sicherheit insbesondere für Betreiber Kritischer Infrastrukturen deutlich an Bedeutung gewonnen. Mit dem IT-Sicherheitskatalog der Bundesnetzagentur wurde für die Gasnetz- und -anlagenbetreiber ein Mindeststandard für die Informationssicherheit verpflichtend vorgegeben. Die Kernforderungen des Sicherheitskatalogs sind hierbei der angemessene Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind, die Einführung eines Informationssicherheits-Managementsystems gemäß DIN ISO/IEC 27001 und dessen Zertifizierung durch geeignete Stellen.

Mit der Einführung eines sogenannten „Information Security Management System“ (ISMS, englisch für „Managementsystem für Informationssicherheit“) wird das Rahmenwerk für die Informationssicherheit vorgegeben und geregelt. In einem ISMS werden hierbei Verantwortlichkeiten, Verfahren und Regeln definiert, die innerhalb der Organisation geeignet sind, die Informationssicherheit dauerhaft zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Diese organisatorischen Regelungen zur Informationssicherheit werden in Richtlinien beschrieben und regeln z. B. die Anforderungen im Umgang mit organisationseigenen Werten, Regelungen zur Sicherheit von Netzwerken, Zugriffsrechten und Kennworten, wie auch Vorgaben zu betrieblichen IT-Prozessen und zur Umsetzung von physischen Sicherheitsmaßnahmen.

Risikoanalyse und Anforderungen des ISMS

Ein zentraler ISMS-Prozess zur kontinuierlichen Sicherstellung und Verbesserung der Informationssicherheit ist eine regelmäßige Risikoanalyse **(Abb. 3)**. Hierbei werden für die Prozesse der Netzsteuerung die kritischen Assets erfasst und hinsichtlich ihres Schutzbedarfs und der relevanten Bedrohungsszenarien bewertet. Unter Berücksichtigung der möglichen Aus-

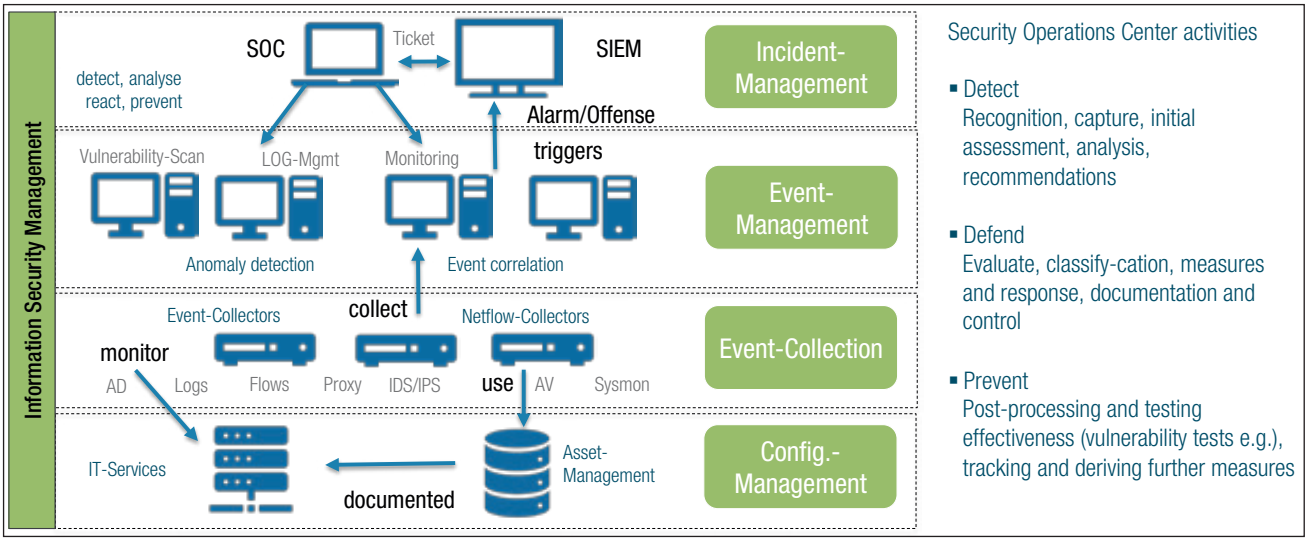


Abb. 4: *Beispiel des Ablaufs in einem Security Incident und Event-Monitoring*

wirkung, z. B. in Bezug auf die Versorgungssicherheit (Business Impact) sowie ihrer Eintrittswahrscheinlichkeit, können risikominimierende Maßnahmen identifiziert und in einen Risikobehandlungsplan überführt, umgesetzt und hinsichtlich ihrer Wirksamkeit bewertet werden.

Das bedeutet beispielsweise für die Leitstellen, dass die Räumlichkeiten, die Dispatcher-Arbeitsplätze sowie die unterstützenden Dienste wie Telefonie- und E-Mail-Kommunikation als Assets erfasst und für diese Werte die Verantwortlichen und die Risikoeigentümer bestimmt werden (siehe Infokasten). Gemeinsam mit den Werte-Verantwortlichen erfolgt die Betrachtung der relevanten Bedrohungsszenarien je Asset und letztlich über die ermittelten Risikowerte, die Ableitung von risikominimierenden Maßnahmen.

BEISPIEL

Unberechtigter Zutritt zum Sicherheitsbereich „Dispatchingzentrale“

Für dieses Bedrohungsszenario empfiehlt sich die folgende Maßnahme: Zutrittsberechtigungen müssen durch den Fachverantwortlichen schriftlich genehmigt werden und werden halbjährlich überprüft. Beim Ausscheiden von Mitarbeitern werden die Berechtigungen (automatisiert) entzogen.

Insbesondere für die Prozesse und Systeme der Netzsteuerung muss die Informationssicherheit die Verfügbarkeit und Integrität der Systeme sicherstellen. Von daher werden, spätestens mit der Einführung eines ISMS, weitere Betriebsprozesse etabliert.

So sollte sichergestellt sein, dass die eingesetzten Betriebssysteme und Applikationen über keine kritischen und angreifbaren Sicherheitslücken verfügen und auch in prozessleitechnischen Netzen regelmäßige Patchprozesse etabliert werden. Mit der Einführung eines technischen Schwachstellenmanagements und regelmäßigen technischen Audits (Penetrationstests) kann die technische Überprüfung von Systemen auf Schwachstellen oder auch Fehlkonfigurationen erfolgen.

Im Gegensatz zu den größtenteils automatisierten Patchprozessen im Umfeld der klassischen IT bedarf es für Systeme der Prozesssteuerung in der Regel abgestimmter Freigabe-Prozesse für das Patchen von Betriebssystemen. Hier haben sich teilautomatisierte Verfahren bewährt, in denen verfügbare Patches zuerst vom Applikationshersteller geprüft und freigegeben werden und dann über eine Softwareverteilung (z. B. WSUS) planmäßig ausgerollt und installiert werden.

Mitunter führen diese Prozesse allerdings dazu, dass wichtige Sicherheits-Updates erst deutlich zeitverzögert oder auch gar nicht eingespielt werden können. Deshalb sollte ein weiteres Augenmerk auf die Systemhärtung und die Netzwerk-Schnittstellen gerichtet sein. Hierbei gilt es insbesondere Verbindungsmöglichkeiten aus anderen Netzsegmenten in Netzbereiche mit hohem Schutzbedarf, wie die der Prozesssteuerung, weitestgehend zu unterbinden und für Zugänge zu Wartungszwecken vorangehende Freischaltungsprozesse zu etablieren.

Mit dem Einsatz eines technischen Schwachstellenmanagements werden Schwachstellen, Fehlkonfigurationen, veraltete Softwareversionen wie auch nur partiell installierte Patches aufgezeigt. Je nach Änderungsaufkommen in den Systemlandschaften ist zu bewerten, ob agentenbasierte oder passive Schwachstellenscanner eingesetzt oder regelmäßig manuelle technische Audits durchgeführt werden.

Weitere Anforderungen aus dem ISMS ergeben sich für die Verwaltung von Benutzerberechtigungen (insbesondere für privilegierte Berechtigungen wie Administratoren-Konten), an die Nachvollziehbarkeit von Änderungsaktivitäten, an das Incident-Management und an eine sichere Aufbewahrung von Logdateien. Für die Stan-

dardbetriebsprozesse wie das Change- und Incident-Management sollte der Einsatz eines Ticket-Systems obligatorisch sein. Sollen perspektivisch weitere Services automatisiert werden, wie beispielsweise die Vergabe von Berechtigungen, empfiehlt sich die Betrachtung einer Servicemanagement-Suite.

Neben den Prozessen im Normalbetrieb sind Vorkehrungen für den Notfall zu treffen und regelmäßig zu proben. Hierzu sollten Umschaltungen auf Ersatzstandorte, die Anwendbarkeit von Notfallplänen, die Beschreibung von Notfallprozessen sowie der Test von Wiederherstellungsprozeduren auf Durchführbarkeit – insbesondere hinsichtlich der geforderten Wiederherstellungszeiten – geprüft werden.

Sind alle diese „Hausaufgaben“ gemacht und die genannten Betriebsprozesse implementiert, so können für die Erkennung von Informationssicherheitsvorfällen Log-Management-Systeme oder ein sogenanntes „Security Incident and Event Management“ (SIEM) zum Einsatz kommen (**Abb. 4**). Neben der „Awareness“ bei den Mitarbeitern, die durch Schulungen, Intranet-Artikel oder auch regelmäßige Phishing-Mails sowie Veranstaltungen zum Thema deutlich gesteigert werden kann, können SIEM-Systeme mit einem umfangreichen Regelwerk versehen werden, um ungewöhnliches Verhalten bzw. Sicherheitsevents zu erkennen und dann Alarm auszulösen. Für die Bearbeitung von Informationssicherheitsvorfällen muss Know-how vorhanden sein; hierzu kann internes Personal aufgebaut als auch ein externes Security Operations Team (SOC) als Dienstleistung bezogen werden.

Abschließende Betrachtung

Um die geschilderten Maßnahmen umsetzen und die ISMS-Prozessen einführen zu können, sind Ressourcen erforderlich. Vor diesem Hintergrund ist die Unterstützung durch das Top-Management eine der wichtigsten Voraussetzungen für ein erfolgreiches ISMS und gleichzeitig eine zentrale Forderung der ISO 27001. Letztlich können technische Sicherheitssysteme wie Firewalls und Anti-Virenschutz-Programme keinen hundertprozentigen Schutz bieten – im Zweifel genügt es einem Angreifer, eine einzige Sicherheitslücke zu finden, um erfolgreich zu sein. Aus diesem Grund sollten regelmäßige Übungen und eine stetige Mitarbeiter-Sensibilisierung zur Informationssicherheit als dauerhafter Prozess etabliert werden.

Zahlreiche etablierte Maßnahmen – angefangen von den physischen Redundanz-Konzepten über eine gute Ausbildung der Mitarbeiter bis hin zu etablierten und zertifizierten Management-Systemen – gewährleisten die Sicherheit der Versorgung der Industrie und der Bevölkerung mit Gas in einem hohen Maß. Aufgrund dieser Vorkehrungen und Normen befinden sich die deutschen Leitstellen und deren Betrieb auf einem hohen Sicherheitsniveau. ■

Literatur

[1] Bundesministerium für Wirtschaft und Energie (Hrsg.): BMWI-Monitoring-Bericht 2017.

[2] www.umweltbundesamt.de/daten/energie/stromverbrauch

[3] Filkins, B., Wylie, D., Dely, J.: SANS 2019 State of OT/ICS Cybersecurity Survey, online unter www.radiflow.com/wp-content/uploads/2019/06/Survey_ICS-2019_Radiflow.pdf, abgerufen am 27. Februar 2020.

Die Autoren

Dr. Werner Rott ist Leiter Gasdisposition bei der GASCADE Gastransport GmbH in Kassel.

Lara Berdelsmann ist Informationssicherheitsbeauftragte bei der GASCADE Gastransport GmbH in Kassel.

Svend Wortmann ist in der Dispatching-Koordination der Nowega GmbH in Münster tätig.

Kontakt:
Dr. Werner Rott
GASCADE Gastransport GmbH
Kölnische Str. 108–112
34119 Kassel
Tel.: 0561 934-1956
E-Mail: werner.rott@gascade.de
Internet: www.gascade.de